Financial Cybercrime Task Force of Kentucky

Technical Alert

Sept. 30, 2014 ***Alert Reference # A0914-01***

Subject: Urgent Alert: Bourne-Again Shell (Bash) ‘Shellshock’ Vulnerability

The DFI’s Financial Cybercrime Task Force of Kentucky (FCTFK) alerts the financial services industry in Kentucky about a material security vulnerability in the Bourne-again shell (Bash) system software widely used in servers and other computing devices. This vulnerability, nicknamed “Shellshock,” could allow attackers to access and gain control of operating systems, exposing organizations and individuals to potential fraud or financial loss, and/or jeopardizing privacy of confidential information.

Background: Bash is a software tool found predominantly on UNIX, Linux, and Mac systems, although it can also be installed on Windows servers. Bash is used to translate user instructions and other inputs into machine-readable commands. Financial institutions may have Bash present on a wide array of servers and network devices, including Web servers, e-mail servers, and physical security systems. The Shellshock vulnerability, reported to be in Bash versions 1.14 through 4.3, could allow a remote attacker to run malware on affected systems.

Recommendations: The Department urges state-chartered financial institutions to immediately take the risk mitigation steps outlined in the FFIEC alert issued on Sept. 26, 2014 (http://www.ffiec.gov/press/PDF/FFIEC_JointStatement_BASH_Shellshock_Vulnerability.pdf), reproduced in part herein as follows:

Financial institutions should take the following steps, as appropriate:

- *Identify all servers, systems, and appliances that use vulnerable versions of Bash and follow appropriate patch management practices, including conducting a vulnerability scan to detect if the patch is installed and testing to ensure a secure and compatible configuration.*

- *Apply mechanisms to filter malicious traffic to vulnerable services such as appropriate Web application firewall signatures.*
- *Monitor systems for malicious or anomalous activity and update signatures for intrusion detection and prevention systems.*
- *Ensure that all third-party service providers are taking appropriate action to identify and mitigate risk and monitor the status of vendors' efforts to address the vulnerability.*
- *Review systems to determine if this vulnerability has been exploited and, if necessary, conduct a forensic examination to determine the potential effects of any breach.*

Financial institutions are encouraged to establish mechanisms for obtaining threat and vulnerability information such as through the United States Computer Emergency Readiness Team (US-CERT) portal at www.us-cert.gov or through the Financial Services Information Sharing and Analysis Center (FS-ISAC) at www.fsisac.com.

If you have any questions regarding this Alert, please contact dfi.reporting@ky.gov.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.